

Congruências

João Nuno Tavares*, Ângela Geraldo†

* Faculdade de Ciências da Universidade do Porto

† CMUP/ Universidade do Porto

CITAÇÃO

Tavares, J. N., Geraldo, A. (2017)
Congruências,
Rev. Ciência Elem., V5(01):070.
doi.org/10.24927/rce2017.070

EDITOR

José Ferreira Gomes
Universidade do Porto

RECEBIDO EM

12 de janeiro de 2013

ACEITE EM

17 de julho de 2013

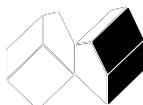
PUBLICADO EM

31 de março de 2017

COPYRIGHT

© Casa das Ciências 2021.
Este artigo é de acesso livre,
distribuído sob licença Creative
Commons com a designação
[CC-BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/), que permite
a utilização e a partilha para fins
não comerciais, desde que citado
o autor e a fonte original do artigo.

rce.casadasciencias.org



Seja m um inteiro positivo. Dois inteiros $a, b \in \mathbb{Z}$ dizem-se congruentes módulo m se a diferença $a-b$ é um múltiplo inteiro de m :

$$a-b=km, \text{ para algum inteiro } k \in \mathbb{Z}$$

Nesse caso escreve-se

$$a \equiv b \pmod{m}$$

Por exemplo

$19 \equiv 5 \pmod{7}$, porque $19-5=14$ é múltiplo inteiro de 7.

$31 \equiv -2 \pmod{3}$, porque $31-(-2)=33$ é múltiplo inteiro de 11.

$12 \equiv 39 \pmod{9}$, porque $12-39=-27$ é múltiplo inteiro de 9.

$16 \equiv -9 \pmod{5}$, porque $16-(-9)=25$ é múltiplo inteiro de 5.

Mas, por exemplo, 3 não é congruente com 11 (mod 7), porque $3-11=-8$ não é múltiplo inteiro de 7.

Propriedades

A propriedade seguinte será usada na dedução dos chamados critérios de divisibilidade.

Teorema

Dois inteiros $a, b \in \mathbb{Z}$ são congruentes módulo m se e só se produzem o mesmo resto quando divididos por m .

Demonstração

Suponhamos que $a \equiv b \pmod{m}$, e que $a=qm+r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < m$. Então $a-b=km, k \in \mathbb{Z}$. Substituindo $a=qm+r$, vem que $b=a-km=qm+r-km=(q-k)m+r$, com $q-k \in \mathbb{Z}$ e $0 \leq r < m$, o que significa que o resto da divisão de b por m também é r .

Reciprocamente, se $a=qm+r$ e $b=q'm+r$ com $q, q', r \in \mathbb{Z}$, $0 \leq r < m$, então $b-a=q'm+r-qm-r=(q'-q)m$, o que significa que $a \equiv b \pmod{m}$, CQD.

Mais propriedades

• Sejam $d, n \in \mathbb{N}$ e $a, b \in \mathbb{Z}$. Temos que:

(i) $a \equiv a \pmod{n}$;

(ii) se $a \equiv b \pmod{n}$, então $b \equiv a \pmod{n}$;

(iii) se $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$, então $a \equiv c \pmod{n}$;

(iv) se $a \equiv b \pmod{n}$ e $d \mid n$ então $a \equiv b \pmod{d}$.

Demonstração

(ii) Se $a \equiv b \pmod{n}$ então $a-b=kn \Leftrightarrow a=b+kn$ com $k \in \mathbb{Z}$. Ora então $b-a=b-(b+kn)=-kn$, ou seja, $b-a$ é um múltiplo inteiro de n e portanto $b \equiv a \pmod{n}$.

(iii) Se $a \equiv b \pmod{n}$ então $a-b=kn \Leftrightarrow a=b+kn$ com $k \in \mathbb{Z}$. Se $b \equiv c \pmod{n}$ então $b-c=tn \Leftrightarrow c=b-tn$ com $t \in \mathbb{Z}$. Ora, $a-c=(b+kn)-(b-tn)=kn+tn=(k+t)n$, ou seja, $a-c$ é um múltiplo inteiro de n , isto é, $a \equiv c \pmod{n}$.

(iv) Se $a \equiv b \pmod{n}$ então $a-b=kn$ com $k \in \mathbb{Z}$. Ora, se $d \mid n$ podemos escrever $n=td$ com $t \in \mathbb{Z}$. Temos então que $a-b=kn=k(td)=(kt)d$, como kt é um número inteiro, concluímos que $a-b$ é um múltiplo inteiro de d , ou seja, $a \equiv b \pmod{d}$.

• Seja $n \in \mathbb{N}$ e sejam a, b, c e $d \in \mathbb{Z}$. Temos que:

(v) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $a+c \equiv b+d \pmod{n}$;

(vi) se $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$, então $ac \equiv bd \pmod{n}$.

Demonstração

(v) Sejam r e s inteiros tais que, $a-b=rn$ e $c-d=sn$. Então, $(a+c)-(b+d)=(a-b)+(c-d)=rn+sn=(r+s)n$, isto é, $(a+c)-(b+d)$ é um múltiplo inteiro de n e portanto $a+c \equiv b+d \pmod{n}$.

(vi) Observemos que $ac-bd=ac-bc+bc-bd=(a-b)c+(c-d)b=rnc+snb=(rc+sb)n$, ou seja, $ac-bd$ é um múltiplo inteiro de n e então $ac \equiv bd \pmod{n}$.